

Updating with VirusScan Enterprise

VERSION 7.0

DOCUMENT REVISION 1.0



COPYRIGHT

© 2003 Networks Associates Technology, Inc. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Networks Associates Technology, Inc., or its suppliers or affiliate companies. To obtain this permission, write to the attention of the Network Associates legal department at: 3965 Freedom Circle, Santa Clara, California 95054, or call +1-972-308-9960.

TRADEMARK ATTRIBUTIONS

Active Firewall, Active Security, Active Security (in Katakana), ActiveHelp, ActiveShield, AntiVirus Anyware and design, Bomb Shelter, Certified Network Expert, Clean-Up, CleanUp Wizard, CNX, CNX Certification Certified Network Expert and design, Design (stylized N), Disk Minder, Distributed Sniffer System, Distributed Sniffer System (in Katakana), Dr Solomon's, Dr Solomon's label, Enterprise SecureCast, Enterprise SecureCast (in Katakana), Event Orchestrator, EZ SetUp, First Aid, ForceField, GMT, GroupShield, GroupShield (in Katakana), Guard Dog, HelpDesk, HomeGuard, Hunter, LANGuru, LANGuru (in Katakana), M and design, Magic Solutions, Magic Solutions (in Katakana), Magic University, MagicSpy, MagicTree, McAfee, McAfee (in Katakana), McAfee and design, McAfee.com, MultiMedia Cloaking, Net Tools, Net Tools (in Katakana), NetCrypto, NetScan, NetShield, NetStalker, Network Associates, NetXray, NotesGuard, Nuts & Bolts, Oil Change, PC Medic, PCNotary, PrimeSupport, Recoverkey, Recoverkey – International, Registry Wizard, ReportMagic, Router PM, Safe & Sound, SalesMagic, SecureCast, Service Level Manager, ServiceMagic, SmartDesk, Sniffer, Sniffer (in Hangul), Stalker, SupportMagic, TIS, TMEG, Total Network Security, Total Network Visibility, Total Network Visibility (in Katakana), Total Service Desk, Total Virus Defense, Trusted Mail, UnInstaller, Virex, Virus Forum, ViruScan, VirusScan, WebScan, WebShield, WebShield (in Katakana), WebSniffer, WebStalker, WebWall, Who's Watching Your Network, WinGauge, Your E-Business Defender, ZAC 2000, Zip Manager are registered trademarks of Network Associates, Inc. and/or its affiliates in the US and/or other countries. All other registered and unregistered trademarks in this document are the sole property of their respective owners.

This product includes or may include software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)

This product includes or may include cryptographic software written by Eric Young. (ey@cryptsoft.com)

LICENSE AGREEMENT

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANIES YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEB SITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO NETWORK ASSOCIATES OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

Preface	5
Audience	5
Getting more information	6
Contacting McAfee and Network Associates	8
1 Introduction	9
Updating tasks and tools	9
Update directory structure	11
2 Repositories	13
Existing customers	14
FTP repository	14
UNC share or local path	15
HTTP repository	15
New customers	16
FTP repository	16
UNC share or local path	17
HTTP repository	18
Configuring HTTP with proxy environments	19
3 Updating Scenarios	21
Updating from the Network Associates repository	22
Multiple sites updating from the Network Associates repository	24
Multiple sites updating internally with a staged deployment	26
4 Managing the AutoUpdate Repository List	29
Sample updating procedure	30
Using VirusScan Enterprise to replicate the update structure	31
Using McAfee Installation Designer	33
Using McAfee AutoUpdate Architect	37
5 Troubleshooting	41

Preface

This Implementation Guide describes the VirusScan Enterprise updating process, and provides the following information:

- Overview of the update process using McAfee AutoUpdate 7.0. See [Update process overview on page 10](#).
- Overview of the update directory structure. See [Update directory structure in the repository on page 11](#).
- Information about specifying repositories for both existing and new customers. See [Repositories on page 13](#).
- Performing updates using different scenarios. These scenarios include using VirusScan Enterprise, McAfee AutoUpdate Architect™, and McAfee Installation Designer™ independently, or in a mixed environment. See [Updating Scenarios on page 21](#).
- Managing the repository list using VirusScan Enterprise, McAfee Installation Designer, and McAfee AutoUpdate Architect. See [Managing the AutoUpdate Repository List on page 29](#).
- Troubleshooting information that applies to updating with VirusScan Enterprise. See [Troubleshooting on page 41](#).
- Roadmap for getting additional information.

This document will be revised periodically to provide the latest updating information. The document revision number is shown on the title page. Document revisions are posted on the Download Site. See [Contacting McAfee and Network Associates on page 8](#) for information about how to access the Download Site.

Audience

This information is intended primarily for two audiences:

- Network administrators who are responsible for their company's anti-virus and security program.
- Users who are responsible for updating virus definition (DAT) files on their workstation, or configuring the software's detection options.

Getting more information

- Product Guide** Product introduction and features, detailed instructions for configuring the software, information on deployment, recurring tasks, and operating procedures.
- Available in an Adobe Acrobat .PDF file from either the product CD or the McAfee download site.
- Several documents are directly referred to in this guide. It is important to have ready access to these documents while performing the activities described in this guide. Refer to the following documents for specific details about each product:
- *VirusScan Enterprise Product Guide*
 - *McAfee Installation Designer Product Guide*
 - *McAfee AutoUpdate Architect Product Guide*
- Installation Guide** System requirements and instructions for installing and starting the software.
- Available as a printed booklet that accompanies the product CD. Also available in an Adobe Acrobat .PDF file from either the product CD or the McAfee download site.
- Help** Product information in the Help system that is accessed from within the application.
- The Help system provides high-level and detailed information. Access from either a Help menu option or Help button in the application.
 - Context-sensitive (*What's This?*) Help provides brief descriptions of the selections in the application. Access by right-clicking on an option, pressing the [F1] control key, or dragging the question icon to an option.
- Release Guide** High-level description of new and changed features for this version of the product.

Configuration Guide	<p><i>For use with ePolicy Orchestrator.</i> Procedures for installing, configuring, deploying, and managing your McAfee product through ePolicy Orchestrator™ management software.</p> <p>Available in an Adobe Acrobat .PDF file from either the product CD or the McAfee download site.</p>
Release Notes	<p><i>README file.</i> Product information, system requirements, resolved issues, any known issues, and last-minute additions or changes to the product or its documentation.</p> <p>Available as a .TXT file from either the product CD or the McAfee download site.</p>
Contact	<p>A list of phone numbers, street addresses, web addresses, and fax numbers for Network Associates offices in the United States and around the world. Also provides contact information for services and resources, including:</p> <ul style="list-style-type: none">■ Technical Support■ Customer Service■ Download Support■ AVERT Anti-Virus Emergency Response Team■ McAfee Beta Site■ On-Site Training■ Network Associates Offices Worldwide

Contacting McAfee and Network Associates

Technical Support:

Service Portal <http://mysupport.nai.com>
<http://knowledge.nai.com>

McAfee Beta Site www.mcafeeb2b.com/beta/

AVERT Anti-Virus
Emergency Response Team www.mcafeeb2b.com/naicommon/avert/default.asp

Download Site www.mcafeeb2b.com/naicommon/download/

DAT File Updates:

HTTP <http://download.nai.com/products/commonupdater>
FTP <ftp://ftp.nai.com/commonupdater>

Product Upgrades www.mcafeeb2b.com/naicommon/download/upgrade/login.asp
Valid grant number required.
Contact Network Associates Customer Service.

On-Site Training www.mcafeeb2b.com/services/mcafee-training/default.asp

Network Associates Customer Service:

E-mail services_corporate_division@nai.com
Web www.nai.com
www.mcafeeb2b.com

US, Canada, and Latin America toll-free:

Phone +1-888-VIRUS NO or +1-888-847-8766
Monday – Friday, 8 a.m. – 8 p.m., Central Time

For additional information on contacting Network Associates and McAfee — including toll-free numbers for other geographic areas — see the Contact file that accompanies this product release.

The VirusScan Enterprise software provides easier, more flexible updating than previous versions of VirusScan and NetShield®. With VirusScan Enterprise you can download updates for both DAT files and scanning engines from the Network Associates repository. A repository, or download site, is a location from which you retrieve updates.

To download a HotFix, a Service Pack, an EXTRA.DAT, a SuperDAT package, or a .CAB file, use the McAfee AutoUpdate Architect utility to check these packages into the AutoUpdate repository.

You can use VirusScan Enterprise, McAfee Installation Designer, or the McAfee AutoUpdate Architect utility to configure and manage various aspects of updating.

VirusScan 4.5.x and NetShield 4.5 allowed updating via FTP, UNC share, or local path. The VirusScan Enterprise 7.0 software adds HTTP to the list.

The information in this document is based on the assumption that you have installed the VirusScan Enterprise software. If you have not installed the software, see the *VirusScan Enterprise Installation Guide*.

The following topics are covered in this section:

- [Updating tasks and tools.](#)
- [Update directory structure on page 11.](#)

Updating tasks and tools

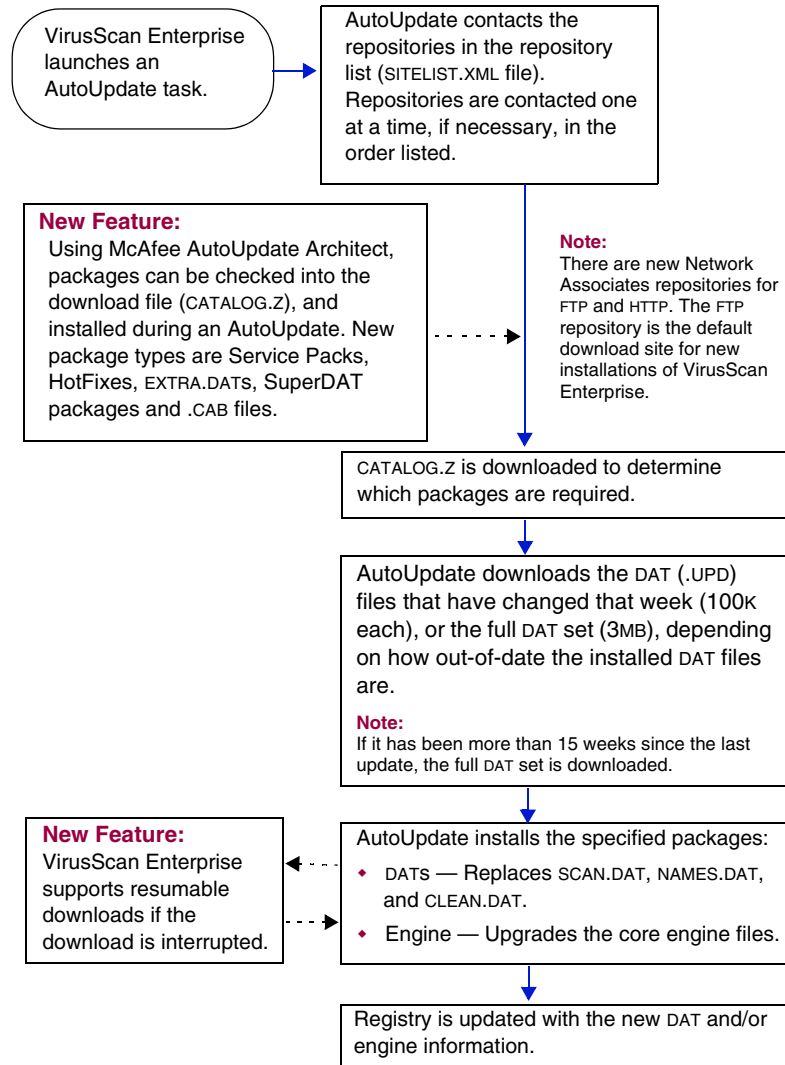
The VirusScan Enterprise software provides two methods for performing updates:

- The AutoUpdate task is used to perform scheduled or immediate updates.
- The Rollback DATs tool is used to roll back the DAT files to the last backed up version.

See the *VirusScan Enterprise Product Guide* for details.

The following provides an overview of the AutoUpdate task and the Rollback DAT files feature.

AutoUpdate Task:



Rollback DAT Files:

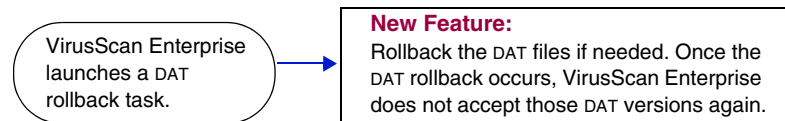


Figure 1-1. Update process overview

Update directory structure

The VirusScan Enterprise software relies on a directory structure to update itself. This directory structure also supports VirusScan 4.5.x and NetShield 4.5 for updating, as long as the entire directory structure is replicated in the same locations that VirusScan 4.5.1 used for updating.

The following shows the directory structure in the repository after using a mirror task to replicate the Network Associates repository.

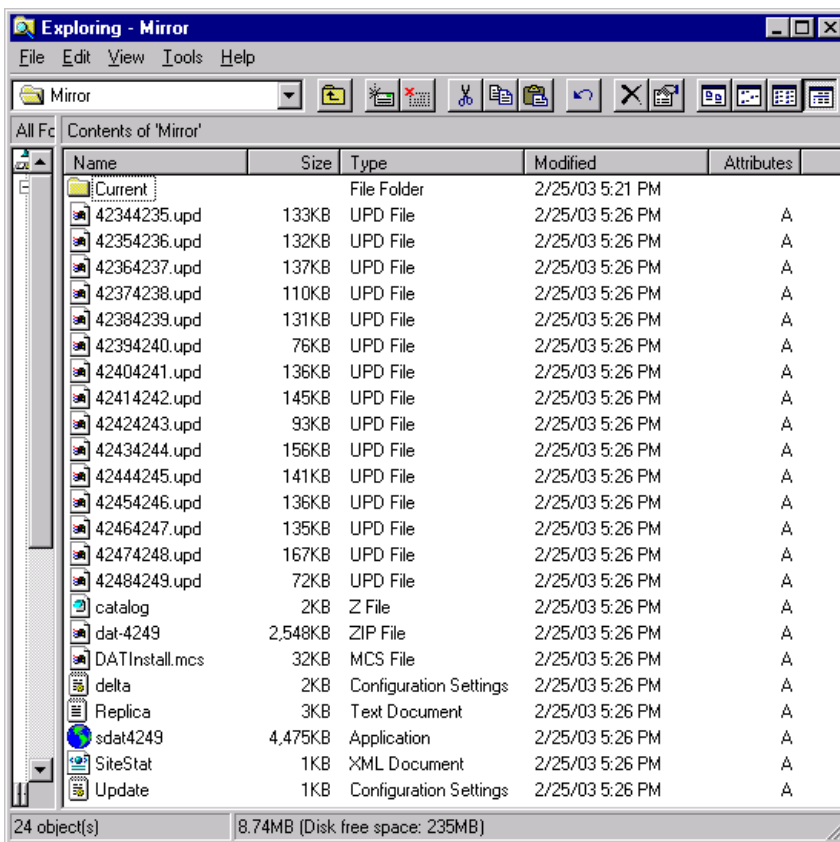


Figure 1-2. Update directory structure in the repository

For more information about the repository directory structure, see [Using VirusScan Enterprise to replicate the update structure on page 31](#).

A repository, or download site, is a location from which you retrieve updates. The repository list, `SITELIST.XML`, contains one or more repositories. The number of repositories that you need depends on your updating requirements. This section describes how existing and new customers can specify repositories.

The VirusScan Enterprise repository list comes pre-configured with two repositories.

- The Network Associates FTP repository is the default download site. It is located at:

```
FTP://FTP.NAL.COM/COMMONUPDATER
```

- The Network Associates HTTP repository is a fallback download site. It is located at:

```
HTTP://DOWNLOAD.NAL.COM/PRODUCTS/COMMONUPDATER
```

See *Editing the AutoUpdate repository list* in the *VirusScan Enterprise Product Guide* for more information about configuring repositories.

You can specify repositories depending on your updating needs as follows:

- [Existing customers on page 14.](#)
- [New customers on page 16.](#)

Existing customers

If you are installing the VirusScan Enterprise 7.0 software over a previous version of VirusScan or NetShield, you can select the **preserve settings** option during installation.

NOTE

When you select the **preserve settings** option, all settings are preserved with one exception. If you had your previous version of VirusScan or NetShield set to update via an FTP repository, and you select the **preserve settings** option during the installation process, the FTP repository location is automatically updated to the new Network Associates FTP repository location that is being used with VirusScan Enterprise.

FTP repository

The default Network Associates FTP repository is located at:

```
FTP://FTP.NAI.COM/COMMONUPDATER
```

The Network Associates FTP repository is the default download site. If you plan to continue to use the FTP repository to perform updates, you are automatically configured to do so after the VirusScan Enterprise 7.0 installation process completes.

UNIX FTP servers as updating or replication servers

Using UNIX FTP servers as updating or replication servers applies to VirusScan Enterprise and McAfee AutoUpdate Architect.

UNIX FTP servers are supported with the following restriction:

- Our updating schema is not aware of relative user paths for the updating and replication accounts. This affects the update path that you configure in VirusScan Enterprise and the replication strategy that you design and manage with McAfee AutoUpdate Architect.

If two separate accounts (such as an anonymous user and an authenticated user) are being used to access the same repository, then the path from the root (/) of the file system to the repository must be the same for both FTP users.

This means that if you execute the *chroot* command on one user, you must execute *chroot* on the other, making sure to use either the same location or symbolic links to that location. Therefore, if anonymous defines the root as `/var/ftp`, then the replicator account's home directory should be `/var/ftp`; and the FTP server should be configured to execute the *chroot* replicator to its home directory.

NOTE

Setting symbolic links is beyond the scope of this document; refer to your UNIX documentation.

UNC share or local path

If you are using a UNC share or a local path to perform updates, and plan to continue doing so, choose from these options:

- **Preserve settings** — Use the Setup utility to install the VirusScan Enterprise software, and select the **preserve settings** option during the installation process.
- **Pre-configuration option** — Use McAfee Installation Designer to modify the .MSI installation file before installing the VirusScan Enterprise software. See the *McAfee Installation Designer Product Guide* for details.
- **Post installation option** — Use McAfee Installation Designer to save your current settings to a .CAB file, then install the VirusScan Enterprise software. After the installation completes, place the .CAB file in the *MID* folder located in the VirusScan Enterprise installation directory. See the *McAfee Installation Designer Product Guide* for details.

HTTP repository

The default Network Associates HTTP repository is located at:

```
HTTP://DOWNLOAD.NAI.COM/PRODUCTS/COMMONUPDATER
```

VirusScan 4.5.x and NetShield 4.5 did not allow updating via an HTTP repository. See [HTTP repository on page 18](#) for information about specifying an HTTP repository.

New customers

If you are installing the VirusScan Enterprise 7.0 software for the first time, you have the following options for specifying repositories:

FTP repository

The default Network Associates FTP repository is located at:

```
FTP://FTP.NAI.COM/COMMONUPDATER
```

The Network Associates FTP repository is the default download site. If you plan to use the FTP repository to perform updates, you are automatically configured to do so after the VirusScan Enterprise 7.0 installation process completes.

UNIX FTP servers as updating or replication servers

Using UNIX FTP servers as updating or replication servers applies to VirusScan Enterprise and McAfee AutoUpdate Architect.

UNIX FTP servers are supported with the following restriction:

- Our updating schema is not aware of relative user paths for the updating and replication accounts. This affects the update path that you configure in VirusScan Enterprise and the replication strategy that you design and manage with McAfee AutoUpdate Architect.

If two separate accounts (such as an anonymous user and an authenticated user) are being used to access the same repository, then the path from the root (/) of the file system to the repository must be the same for both FTP users.

This means that if you execute the *chroot* command on one user, you must execute *chroot* on the other, making sure to use either the same location or symbolic links to that location. Therefore, if anonymous defines the root as */var/ftp*, then the replicator accounts home directory should be */var/ftp*; and the FTP server should be configured to chroot replicator to its home directory.

NOTE

Setting symbolic links is beyond the scope of this document; refer to your UNIX documentation.

UNC share or local path

If you plan to perform updates using a UNC share or a local path, you must install the VirusScan Enterprise software, then configure the UNC share or the local path in the AutoUpdate repository list. See *Editing the AutoUpdate repository list* in the *VirusScan Enterprise Product Guide* for details.

After you have installed the VirusScan Enterprise software and configured the UNC share, you have these configuration options for future installations of VirusScan Enterprise:

- **Pre-configuration option** — Use McAfee Installation Designer to modify the .MSI installation file with the UNC settings, and use this file to ensure all future VirusScan Enterprise installations use those UNC settings. See the *McAfee Installation Designer Product Guide* for details.
- **Post installation option** — Use McAfee Installation Designer to create a .CAB file that specifies the UNC settings. Use the .CAB file for all future VirusScan Enterprise installations that are to be configured with the UNC settings. See the *McAfee Installation Designer Product Guide* for details.

NOTE

We strongly recommend that you test any configuration process before using it for deployment.

HTTP repository

The default Network Associates HTTP repository is located at:

HTTP://DOWNLOAD.NAI.COM/PRODUCTS/COMMONUPDATER

If you plan to perform updates using an HTTP repository, you must install the VirusScan Enterprise software, then configure the HTTP repository in the AutoUpdate repository list. See *Editing the AutoUpdate repository list* in the *VirusScan Enterprise Product Guide* for details.

After you have installed the VirusScan Enterprise software and configured the HTTP repository, you have these configuration options for future installations of VirusScan Enterprise:

- **Pre-configuration option** — Use McAfee Installation Designer to modify the .MSI installation file with the HTTP settings, and use this file to ensure all future VirusScan Enterprise installations use those HTTP settings. See the *McAfee Installation Designer Product Guide* for details.
- **Post installation option** — Use McAfee Installation Designer to create a .CAB file that specifies the HTTP settings. Use the .CAB file for all future VirusScan Enterprise installations that are to be configured with the HTTP settings. See the *McAfee Installation Designer Product Guide* for details.

NOTE

We strongly recommend that you test any configuration process before using it for deployment.

Configuring HTTP with proxy environments

VirusScan Enterprise 7.0 uses the proxy settings for the locally installed version of Internet Explorer 4.0 or higher, to authenticate to the proxy server. If you configure VirusScan Enterprise to use the HTTP repository, it is important to consider the following situations when you are designing your update strategy:

- **Multiple authentications with proxy and firewalls** — VirusScan Enterprise 7.0 cannot update if your environment needs to authenticate to more than one device, such as to a proxy server and a firewall. The update may appear to take longer than expected, and time out with the following error:

Cannot Authenticate to Proxy server error or Access denied - You are not permitted to see this page error.

- **Content-scanning firewalls** — Some content-scanning firewall programs include an option to scan incoming traffic for non-business related material. Network Associates has implemented security checks to monitor whether our download files have been modified in any way and are valid. Most content-scanning firewalls that were tested do *not* modify our packages during download. If the content-scanning firewall does modify the Network Associates packages, you may see an *Unable to open files* error, or other errors depending on what was changed about our files. If possible, you should configure the content-scanning firewall program so that it does *not* scan the Network Associates download site.

You can use several updating methods, depending on your environment and updating needs.

Refer to the following update scenarios for information about updating in your environment:

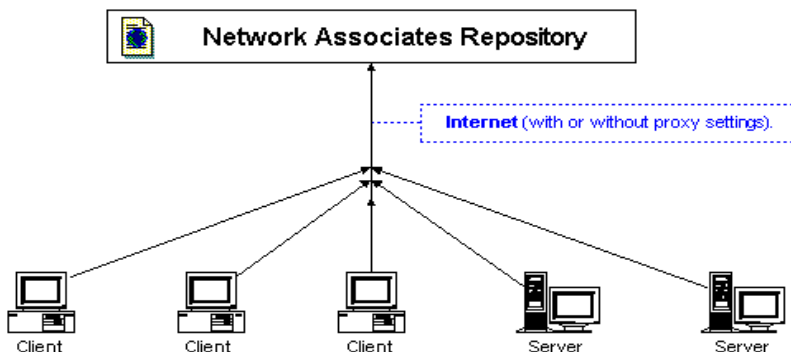
- *Updating from the Network Associates repository on page 22.*
- *Multiple sites updating from the Network Associates repository on page 24.*
- *Multiple sites updating internally with a staged deployment on page 26.*

Updating from the Network Associates repository

Use this scenario for updating DAT and engine files from the Network Associates repository.

NOTE

To download HotFix, Service Pack, EXTRA.DAT, SuperDAT package, or .CAB files, see [Using McAfee AutoUpdate Architect on page 37](#).



Assumption: Clients and servers are configured to update once per week.

Figure 3-1. Updating from the Network Associates repository

- **Pre-configuration options** — Use McAfee Installation Designer to customize the VirusScan Enterprise 7.0 installation package (.MSI file). If you do so, the new defaults take effect when you install the VirusScan Enterprise software to other computers.

See the *McAfee Installation Designer Product Guide* for details.

- **FTP repository** — The Network Associates FTP repository is the default download site. If you are currently using the default VirusScan 4.5.1 FTP repository, or plan to use the FTP repository to perform updates after installing VirusScan Enterprise 7.0, you are automatically configured to do so after the installation process completes. No changes are required to the VirusScan Enterprise 7.0 installation package (.MSI file).

The default Network Associates FTP repository is located at:

```
FTP://FTP.NAI.COM/COMMONUPDATER
```

If you are installing VirusScan Enterprise over a previous version of VirusScan or NetShield, and wish to *preserve settings*, select the **preserve settings** option during installation.

NOTE

If you are currently using the default VirusScan 4.5.1 FTP repository, VirusScan Enterprise automatically updates to the new default FTP repository, even if you choose to **preserve settings**.

- **HTTP repository or internal UNC share** — Use McAfee Installation Designer to configure these repositories before or after installing VirusScan Enterprise.

See the *McAfee Installation Designer Product Guide* for details.

The default Network Associates HTTP repository is located at:

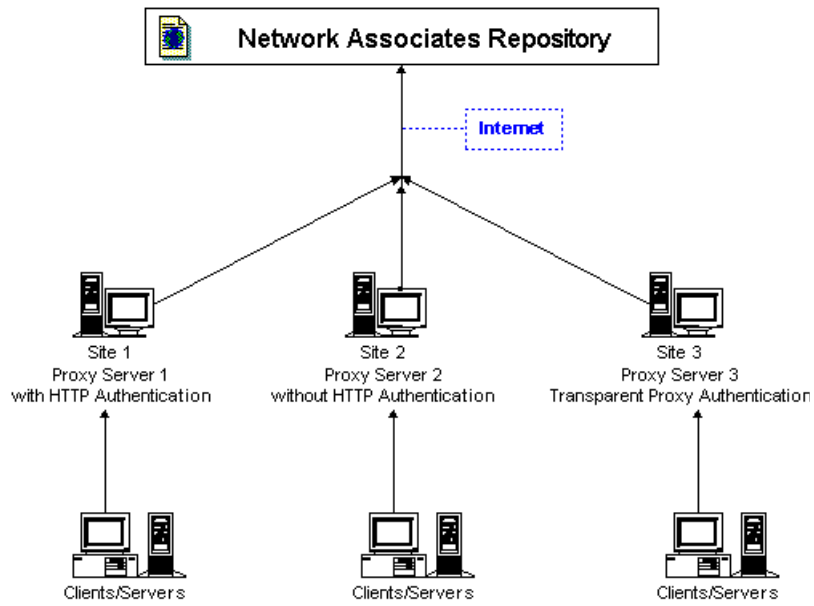
```
HTTP://DOWNLOAD.NAI.COM/PRODUCTS/COMMONUPDATER
```

Multiple sites updating from the Network Associates repository

Use this scenario for updating DAT and engine files, for multiple sites, from the Network Associates repository.

NOTE

To download HotFix, Service Pack, EXTRA.DAT, SuperDAT package, or .CAB files, see [Using McAfee AutoUpdate Architect on page 37](#).



Assumption: Clients and servers are configured to update once per week.

Figure 3-2. Multiple sites updating from the Network Associates repository

- **Pre-configuration options** — Use McAfee Installation Designer to customize the VirusScan Enterprise 7.0 installation package (.MSI file). If you do so, the new defaults take effect when you install the VirusScan Enterprise software to other computers.

See the *McAfee Installation Designer Product Guide* for details.

- **FTP repository** — The Network Associates FTP repository is the default download site. If you are currently using the default VirusScan 4.5.1 FTP repository, or plan to use the FTP repository to perform updates after installing VirusScan Enterprise 7.0, you are automatically configured to do so after the installation process completes. No changes are required to the VirusScan Enterprise 7.0 installation package (.MSI file).

The default Network Associates FTP repository is located at:

FTP://FTP.NAI.COM/COMMONUPDATER

If you are installing VirusScan Enterprise over a previous version of VirusScan or NetShield, and wish to *preserve settings*, select the **preserve settings** option during installation.

NOTE

If you are currently using the default VirusScan 4.5.1 FTP repository, VirusScan Enterprise automatically updates to the new default FTP repository, even if you choose to **preserve settings**.

- **HTTP Network Associates repository or internal UNC share** — Use McAfee Installation Designer to configure these repositories before or after installing VirusScan Enterprise.

See the *McAfee Installation Designer Product Guide* for details.

The default Network Associates HTTP repository is located at:

HTTP://DOWNLOAD.NAI.COM/PRODUCTS/COMMONUPDATER

- **HTTP authentication** — Site 1 uses authentication and the other two sites do not. There are several ways to plan for this configuration:

- ◆ Use ePolicy Orchestrator™ or McAfee AutoUpdate Architect to manage this site configuration.

See the *ePolicy Orchestrator Product Guide* or the *McAfee AutoUpdate Architect Product Guide* for details.

- ◆ Use McAfee Installation Designer to create two .CAB files that contain the required site-specific update information. Copy these .CAB files to the MID folder located in the VirusScan Enterprise installation directory. VirusScan Enterprise retrieves the site settings from the .CAB files and uses it for updating.

You can also use McAfee Installation Designer to create workstation-specific or server-specific .CAB files.

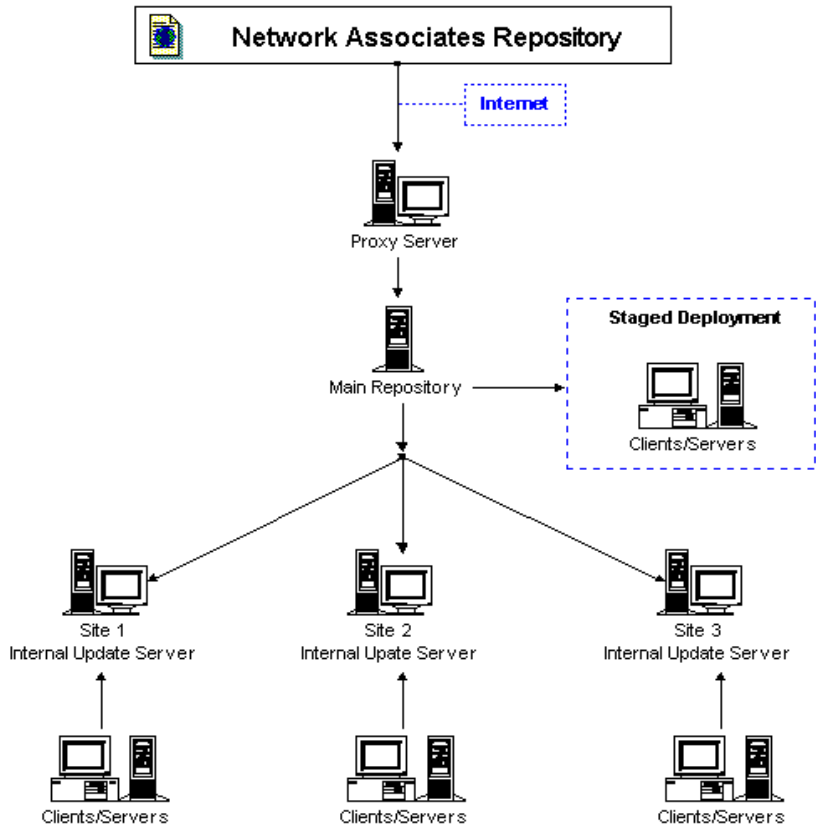
See the *McAfee Installation Designer Product Guide* for details.

- ◆ Use McAfee Installation Designer to create two installation packages; one for each site that contains the required site-specific updating information. As each package deploys, it configures the local computer to use the site-specific update information, such as proxy user name and password, or proxy IP address.

See the *McAfee Installation Designer Product Guide* for details.

Multiple sites updating internally with a staged deployment

Use this scenario to test deployment before replicating the update files to the internal servers:



Assumption: Clients and servers are configured to update once per week.

Figure 3-3. Multiple sites updating internally with a staged deployment

In this scenario, a staged deployment site has been created for a limited number of users to test the DAT files, before deploying them to the remainder of the company. A main repository is configured to retrieve updates from the Network Associates FTP or HTTP repository.

You can create the main repository using either of these options:

- Use the VirusScan Enterprise *mirror* task to replicate the Network Associates repository to the main repository. See the *VirusScan Enterprise Product Guide* for details about using the mirror task.
- Use the McAfee AutoUpdate Architect *pull* task. See the *McAfee AutoUpdate Architect Product Guide* for details about using the pull task.

Once the update structure is in place, test clients and servers that are configured to update from this main repository, will do so when their next scheduled update runs.

NOTE

McAfee AutoUpdate Architect can check Service Packs, HotFixes, EXTRA.DATS, SuperDAT packages, and .CAB file packages into this update structure, so that the VirusScan Enterprise update task pulls these packages down and installs them during scheduled updates.

After the testing cycle is complete, the structure can be replicated to the internal servers for the remainder of the company. You can use the command line or common scripting utilities to manage replication. McAfee AutoUpdate Architect can manage and automate these replication tasks from the Network Associate repository to the main repository, as well as from the main repository to the internal update servers. The internal servers can be FTP, HTTP, or UNC shares.

Managing the AutoUpdate Repository List

4

The AutoUpdate repository list contains the repositories used to perform update tasks. You can have as many repositories as you need to meet your updating requirements. You can use the AutoUpdate repository list to download the following:

- DAT file updates
- Scanning engine upgrades
- EXTRA.DAT file
- SuperDAT package
- HotFix
- Service Pack
- .CAB file

You can use VirusScan Enterprise, McAfee Installation Designer, the McAfee AutoUpdate Architect utility, or a combination of these tools to manage the AutoUpdate repository list.

The tools you select to manage the AutoUpdate repository list, depend on your updating requirements.

The following topics are covered in this section:

- [Sample updating procedure on page 30.](#)
- [Using VirusScan Enterprise to replicate the update structure on page 31.](#)
- [Using McAfee Installation Designer on page 33.](#)
- [Using McAfee AutoUpdate Architect on page 37.](#)

Sample updating procedure

The following procedure lists the basic steps required to perform an update:

- 1 Configure the VirusScan Enterprise 7.0 installation (.MSI) package to download from a repository.
 - a If you are updating from the default Network Associates FTP repository, no changes need to be made to the installation package.
 - b If you are updating from either of the following repositories, you can configure the installation package:
 - ◆ Network Associates HTTP repository as the main repository.
 - ◆ Internal FTP, HTTP, or UNC/mapped drive as the repository.

Use McAfee Installation Designer to pre-configure the installation package, or configure VirusScan Enterprise after installation.

See the *McAfee Installation Designer Product Guide* for details.

- 2 For clients updating to an internal update server:
 - a Mirror the update structure from either the Network Associates FTP repository or the HTTP repository, to the internal update location on your server. You can use the VirusScan Enterprise mirror task on a single server, to replicate these files from the repository to a location on that server.

See the *VirusScan Enterprise Product Guide* for more information about using mirror tasks.

NOTE

The files located on the Network Associates FTP repository and the HTTP repository support both VirusScan 4.5.x and VirusScan Enterprise 7.0.

- b Copy the update structure to the other internal update servers. You may already have an existing method for copying the update files to other internal servers. You can use any existing methods, as long as the entire directory structure is replicated.

You can use McAfee AutoUpdate Architect to manage and automate this process. See the *McAfee AutoUpdate Architect Product Guide* for details.

- 3 Deploy the VirusScan Enterprise 7.0 installation package to your environment. The installation package should be configured to update to the prepared internal download site, or the external download site.

Using VirusScan Enterprise to replicate the update structure

You can create a mirror task in VirusScan Enterprise, and use it to replicate update files to a mirror location. See the *VirusScan Enterprise 7.0 Product Guide* for details about using mirror tasks.

- 1 Start the **VirusScan Console**.
- 2 Create a new mirror task or open an existing mirror task.

The **VirusScan AutoUpdate Properties** dialog box appears.

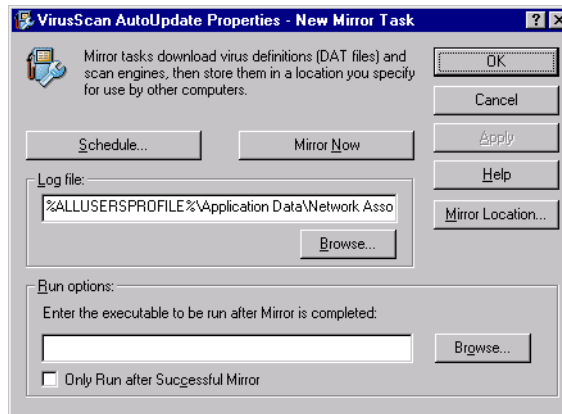


Figure 4-1. VirusScan AutoUpdate Properties — Mirror task

- 3 Click **Mirror Location**.
 - a In the **Local Destination Path** text box, enter the mirror location, or click **Browse** to navigate to the desired location.
 - b Click **OK** to return to the **VirusScan AutoUpdate Properties** dialog box.
 - c Click **Mirror Now** to start the mirror task.
 - d Click **OK** to close the **VirusScan AutoUpdate Properties** dialog box and return to the **VirusScan Console**.
- 4 Monitor the task progress on the **VirusScan Console**.

Each mirror site replicates the Network Associates repository that contains the update files. Computers on your network can then download the files from the mirror site. This approach is practical because it allows you to update any computer on your network, whether or not it has Internet access. It is also efficient because your computers communicate with a server that is probably closer than a Network Associates Internet site, therefore economizing access and download time. The most common use of this task is to *mirror* the contents of the Network Associates repository to a local server.

The VirusScan Enterprise software relies on a directory structure to update itself. This directory structure also supports VirusScan 4.5.x and NetShield 4.5 for updating, as long as the entire directory structure is replicated in the same locations that VirusScan 4.5.1 used for updating.

The following shows the directory structure in the repository after using a mirror task to replicate the Network Associates repository.

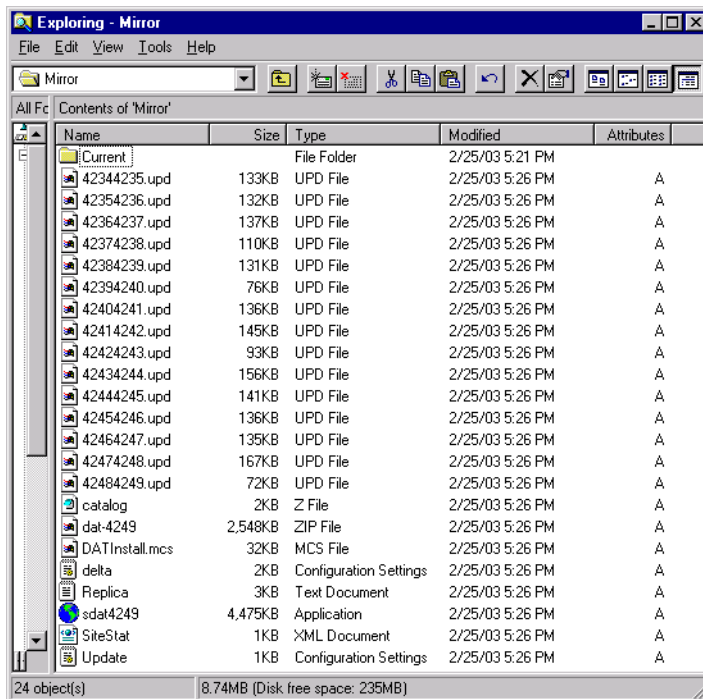


Figure 4-2. Update directory structure in the repository

The mirror task used for this example downloads from the default FTP site, so only the CATALOG.Z file, the DAT file updates, and the engine file were downloaded.

- The files listed in the flat structure of the diagram are used with previous versions of VirusScan and NetShield.
- The CATALOG.Z file and the files contained in the *Current* folder are used with VirusScan Enterprise 7.0.

NOTE

To download a HotFix, a Service Pack, an EXTRA.DAT, a SuperDAT package, or a .CAB file, use the McAfee AutoUpdate Architect utility to check these packages into the AutoUpdate repository list. See [Using McAfee AutoUpdate Architect on page 37](#) for more information.

Using McAfee Installation Designer

McAfee Installation Designer allows an administrator to pre-configure a VirusScan Enterprise software package for installation on another computer or group of computers.

You can use the utility to:

- Pre-set installation options for VirusScan Enterprise.
- Select additional files to copy to the system during installation.
- Set registry keys in addition to those set by the installation.
- Install the most current DAT and engine files, rather than those that shipped with the product.

Use McAfee Installation Designer to create a .CAB file that modifies an existing VirusScan Enterprise installation. See the *McAfee Installation Designer Product Guide* for details.

- 1 Start the McAfee Installation Designer utility.

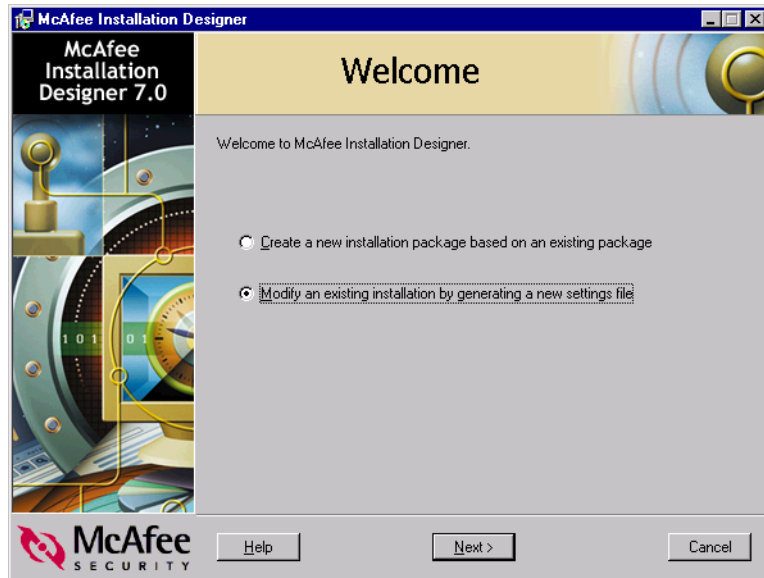


Figure 4-3. McAfee Installation Designer — Welcome

- 2 Select **Modify an existing installation by generating a new settings file**, then click **Next**.

The **Source for Configuration** dialog box appears.

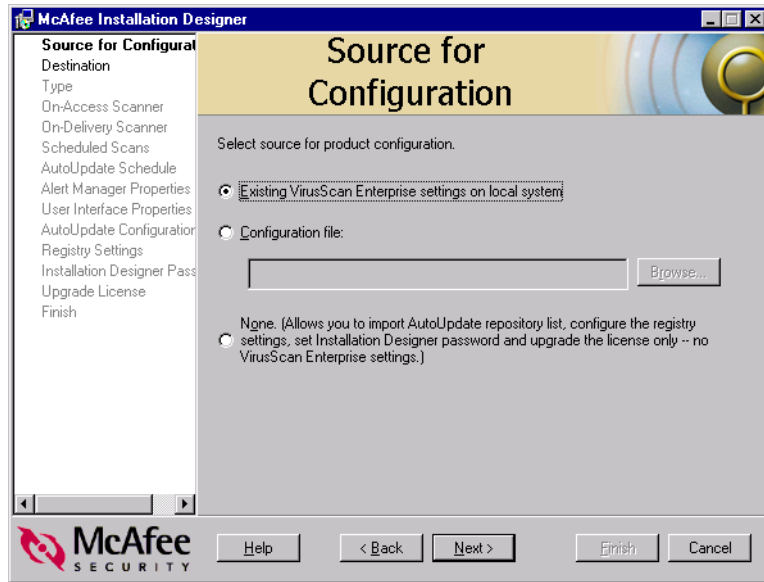


Figure 4-4. McAfee Installation Designer — Source for Configuration

- 3 Select **Existing VirusScan Enterprise settings on local system**, then click **Next**.

The **Destination** dialog box appears.

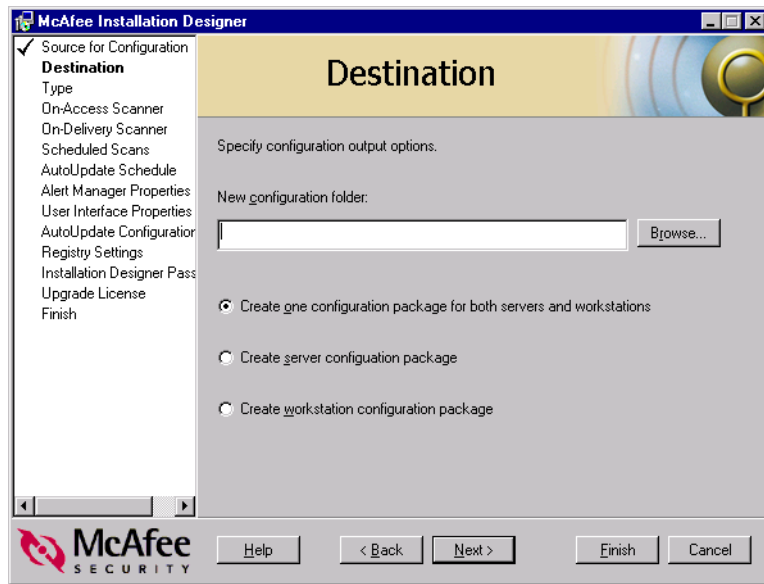


Figure 4-5. McAfee Installation Designer — Destination

- 4 Specify the options for the configuration folder:
 - a In the **New configuration folder** text box, specify the destination for the configuration folder.
 - b Select one of these options:
 - ◆ **Create one configuration package for both servers and workstations.**
 - ◆ **Create server configuration package.**
 - ◆ **Create workstation configuration package.**
- 5 To continue, choose from these options:
 - ◆ Click **Next** to continue through the list of options shown in the left panel.
 - ◆ Click **Finish** at any time to review the final configuration.
- 6 Click **Save** then click **Exit**.

NOTE

After the installation completes, place the .CAB file in the *MID* folder located in the VirusScan Enterprise installation directory.

Using McAfee AutoUpdate Architect

McAfee AutoUpdate Architect allows you to manage updates to your entire company's anti-virus software. The program creates and maintains an internal software repository where you define exactly which Network Associates updates to deploy to the computers on your network.

Using McAfee AutoUpdate Architect, you can configure an FTP server, HTTP server, or a UNC shared directory on your internal network to process all AutoUpdate requests from your network client computers. Those client computers then retrieve their updates from an internal location, rather than connecting directly to the McAfee web site. This reduces bandwidth consumption and allows faster update transfers.

McAfee AutoUpdate Architect task scheduling features allow you to retrieve the latest anti-virus software updates automatically from the Network Associates repository, and store them on your internal update server. Your internal update server can then deliver those updates to distributed repositories throughout your organization.

You can use VirusScan Enterprise along with McAfee AutoUpdate Architect to download the most current update files.

- Use the VirusScan Enterprise AutoUpdate task to download the most current DAT file updates and engine upgrades from the Network Associates repository.
- Use the McAfee AutoUpdate Architect utility to download a HotFix, a Service Pack, an EXTRA.DAT, a SuperDAT package, or a .CAB file, then check these packages into the AutoUpdate repository list.

Use McAfee AutoUpdate Architect to check package files into the AutoUpdate repository list. See the *McAfee AutoUpdate Architect Product Guide* for details.

- 1 Start the McAfee AutoUpdate Architect utility.

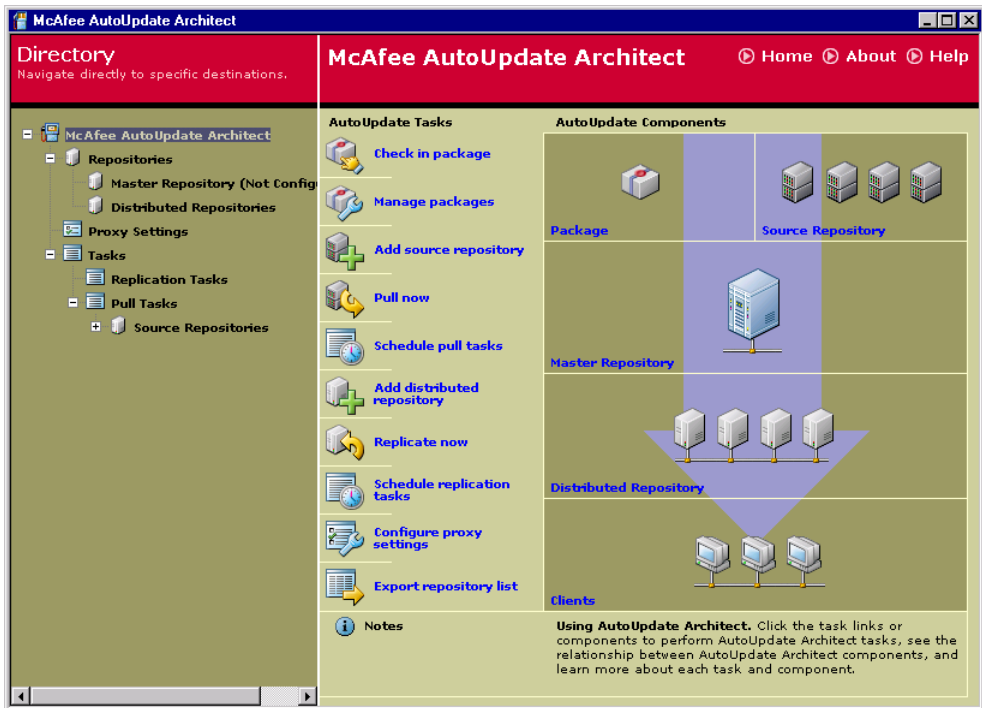


Figure 4-6. McAfee AutoUpdate Architect — Console

- 2 Configure the **Master Repository**, if you have not already done so. See the *McAfee AutoUpdate Architect Product Guide* for details.
- 3 In the console tree, select **McAfee AutoUpdate Architect**, then in the **AutoUpdate Tasks** area, click **Check-in package**.

The **check-in package wizard** dialog box appears.

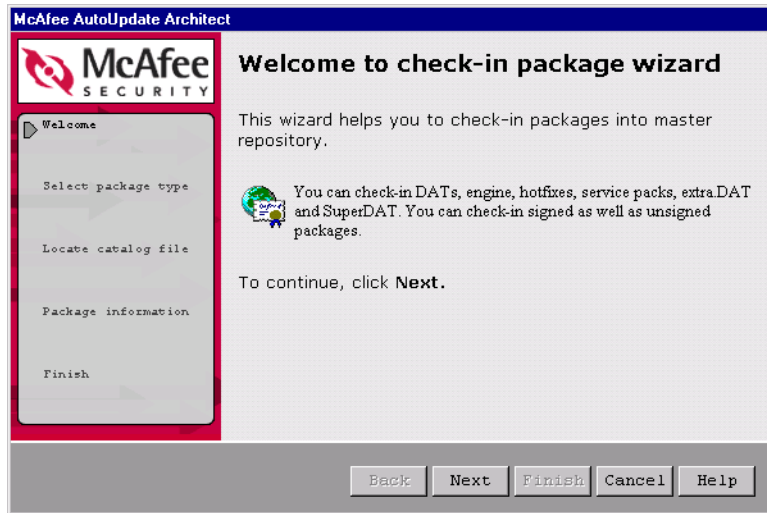


Figure 4-7. McAfee AutoUpdate Architect — Check-in package wizard

- 4 Click **Next** to continue.
- 5 Enter the appropriate information as required, in each of the following dialog boxes:
 - ◆ **Select package type**
 - ◆ **Locate catalog file**
 - ◆ **Package information**
 - ◆ **Finish**

McAfee AutoUpdate Architect verifies the authenticity and integrity of updates, through the use of digital package signatures, to protect against unauthorized modification, tampering, or corruption.

See the *McAfee AutoUpdate Architect Product Guide* for detailed information on configuring and using the utility.

This section contains troubleshooting information for updating with VirusScan Enterprise.

The following topics are covered in this section:

- *Using the AutoUpdate log file to troubleshoot updating issues on page 42.*
- *AutoUpdate may require Internet Explorer 4.0 or later on page 42.*
- *Download catalog.z. on page 43.*
- *DAT file updates using VirusScan 4.5.1 and VirusScan Enterprise 7.0 on page 43.*

Using the AutoUpdate log file to troubleshoot updating issues

To view the AutoUpdate log file, right-click the AutoUpdate task in the **VirusScan Console**, and select **View Log**. You can see basic updating information, general errors, and other configuration errors. Network Associates also provides an alternate log file that provides more advanced logging and HTTP responses, from the HTTP proxy or servers.

The alternate log file name is AGENT_<COMPUTER NAME>.LOG.

The AGENT_<COMPUTER NAME>.LOG file can be found at the following locations, depending on your operating system:

- **For Windows NT 4.0** — In the VirusScan Enterprise installation directory. By default, Setup installs the VirusScan Enterprise program files to this path:

<DRIVE>:\PROGRAM FILES\NETWORK ASSOCIATES\VIRUSSCAN

- **For Windows 2000 and Windows XP** — In the All Users Profile at the following location:

\DOCUMENTS AND SETTINGS\ALL USERS\APPLICATION DATA\NETWORK ASSOCIATES\COMMON FRAMEWORK\DB

NOTE

The *Application Data* folder is hidden by default. If you do not have rights to *Show hidden files and folders*, you cannot view or search for the AGENT_<COMPUTER NAME>.LOG.

AutoUpdate may require Internet Explorer 4.0 or later

Server installations that do not have Microsoft Internet Explorer version 4.0 or later must use McAfee Installation Designer to install the WININET.DLL and the SHLWAPI.DLL. Refer to Primus Article Number 30063.

Download catalog.z.

To test whether you can download the CATALOG.Z file, try using the following methods:

- **If you are using the Network Associates HTTP repository for updates:**

- ◆ HTTP — In the web browser, go to the following URL and try to download the CATALOG.Z file:

```
HTTP://DOWNLOAD.NAI.COM/PRODUCTS/COMMONUPDATER/
CATALOG.Z
```

- **If you are using the Network Associates FTP repository for updates:**

- ◆ FTP — In the web browser, go to the following URL and try to download the CATALOG.Z file:

```
FTP://FTP.NAI.COM/COMMONUPDATER/CATALOG.Z
```

If you are asked to log on, use the following credentials:

User name = anonymous

Password = your e-mail address

If you are *not* able to download the file, but you can see it (in other words, your browser does not allow you to download it), that means you have a proxy issue and need to talk to your network administrator.

If you *are* able to download the file, VirusScan Enterprise 7.0 should be able to download it as well. Contact technical support for assistance in troubleshooting your installation of VirusScan Enterprise.

NOTE

If you are using a mirror site for updates, make sure that your mirror site is pointing to the correct repository for updates. If you are unsure, try changing your settings to use the default Network Associates repository.

DAT file updates using VirusScan 4.5.1 and VirusScan Enterprise 7.0

If you have computers that will continue using VirusScan 4.5.x and others using VirusScan Enterprise 7.0, all of these computers can download the most current DAT files from the same Network Associates repository.

The default Network Associates HTTP repository is located at:

```
HTTP://DOWNLOAD.NAI.COM/PRODUCTS/COMMONUPDATER/
```

The default Network Associates FTP repository is located at:

```
FTP://FTP.NAI.COM/COMMONUPDATER/
```

